FORTINET
High Performance Network Security

FortiAuthenticator - Release Notes

VERSION 5.1.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

11/01/2017

FortiAuthenticator 5.1.0 - Release Notes

Revision 1

TABLE OF CONTENTS

Introduction

This document provides a summary of new features, enhancements, support information, installation instructions and caveats, resolved and known issues for FortiAuthenticator™ 5.1.0, build 0083.

FortiAuthenticator is a User and Identity Management solution that provides Strong Authentication, Wireless 802.1X Authentication, Certificate Management, and Fortinet Single Sign-On.

For additional documentation, please visit:

http://docs.fortinet.com/fortiauthenticator/

Special Notices

TFTP boot process

The TFTP boot process erases all current FortiAuthenticator configuration and replaces it with the factory default settings.

Monitor settings for web-based manager access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the Web-based Manager to be viewed properly without need for scrolling.

Before any upgrade

Save a copy of your FortiAuthenticator unit configuration prior to upgrading. Go to *System* > *Dashboard* > *Status* and select *Backup/Restore* > *Download backup file* to backup the configuration.

After any upgrade

If you are using the Web-based Manager, clear your browser cache prior to login on the FortiAuthenticator to ensure the Web-based Manager screens are displayed properly.

What's New

Before upgrading, review the following changes for impact to your unique deployment. Note that this list is not exhaustive but highlights the major feature enhancements in this release.

Note that this is a patch release which fixes a few issues found in the release of 5.0.0. See Resolved Issues for the issues addressed in this patch release.

For more detailed information, see the FortiAuthenticator 5.1.0 Administration Guide.

New features include:

FSSO: Update group cache (435530) (435591)

A new refresh/update group information feature has been introduced. Once a user's group membership changes, the particular user's information can be manually updated by selecting the button, in an effort to update the user's group information right away. This will not require the user logging off and back on.

NTLM performance (437004) (443951)

NTLM performance has been improved by supporting simultaneous usage of multiple DCs to process authentication, allowing as many as 300 authentications per second with three DCs.

Remote LDAP: Oracle ODSEE support (412856)

Oracle-based ODSEE LDAP support has been enhanced. When the remote LDAP server is Oracle ODSEE, the group search is not allowed unless the LDAP bind is done using the administrator credentials. We added a new option to the remote LDAP server configuration to indicate whether the group filter search must be done using the administrator bind (disabled by default).

Guest Portals: Menu change and customization

Many of the pre-login replacement messages for Guest Portals in FortiAuthenticator 5.0.0 are shared with the Self-service Portal. This meant that customization of those replacement messages applied to both portals. In order to decouple these features, a number of replacement messages have been added to the Guest Portals list of replacement messages.

The post-login page for users of the Guest Portal was also similar to the Self-service's Portal page, with a menu sidebar on the left and the selected menu page on the right. In 5.1.0, the left sidebar has been removed in the effort to make it similar to the social login portal.

Once logged into the Guest Portal, users will have the opportunity to edit their profile (including name, email address, phone number, and address), configure password recovery options (including a change their password, and setup a security question), and register a FortiToken. These options can be made visible to the user or not by configuring *Post-login Services* under *Authentication* > *Guest Portals* > *Portals*.

Guest Portals: FortiWLC support

Guest Portals now includes support for the Meru Connect (support which already existed for Captive Portal). This allows the FortiAuthenticator to auto-detect when requests are coming from the Meru Connect, so no new configuration settings are required in the GUI.

SAML IdP: Support new attributes for assertions (445274)

New assertion user attributes (including FirstName, LastName, and Remote LDAP Group) are now available to return to a Service Provider (SP) when configuring the SAML IdP service under *Authentication* > *SAML IdP* > *Service Providers*.

SAML IdP: Office365 support (423462)

Integration with Office 365 and Windows Azure AD requires a unique identifier for each user in the user directory. Windows Azure AD Service refers to this as the ImmutableID, which typically can be set to the ObjectGUID attribute. This new attribute is available when configuring *Assertion Attributes* under *Authentication* > *SAML IdP* > *Service Providers*.

Guest Portals: 2FA and single NAS support

Guest Portals now support user's ability to enter their FortiToken code upon Guest Portal login (this includes push token and WLC support).

Note: Two-factor authentication is *not* supported for Guest Portal with FortiCloud.

FSSO: Multiple group support for Syslog (416541)

The *Syslog Matching Rules*, under *Fortinet SSO Methods* > *SSO* > *Syslog Sources*, now have a *Group list separator* option. Before now, the SSO syslog feed could only parse multiple groups if the names were separated by a plus (**+**) symbol. Support has been added for commas (**,**) also.

Strong Crypto (401581)

A configurable option to require strong cryptography is now available under *System* > *Administration* > *System Access*. Enable this option to restrict administrative access using stronger cryptographic algorithms, such as TLS 1.2, DHE, AES, and SHA256.

MAC device filtering

New MAC device filtering can be configured in *Device Authentication* under *Authentication* > *RADIUS Service* > *Clients*, where MAC address attributes, authorized groups, and action to take for unauthorized devices can be determined. The *MAC address attribute* indicates which RADIUS attribute to extract the MAC address from.

Note that authorized groups must be first created under *Authentication* > *User Management* > *User Groups*, where *Type* must be set to *MAC*, and MAC devices are selected for MAC address authorization. These can then be referenced in the RADIUS client configuration page, where they are now mandatory.

MAC device filtering can be enabled for any RADIUS authentication, including Guest Portal authentication. However, when used for Guest Portals, the FortiAuthenticator needs to know which HTTP parameter to extract the MAC address from. You can now enter the *MAC device HTTP parameter* under the *Authentication* > *Guest Portals* > *Portals* configuration page.

API: Independent access control (414153)

Access rights have been modified, under *System* > *Network* > *Interfaces*, to allow independent control for GUI administrator and REST API access via HTTPS.

Samba upgrade (414084)

Server Message Block version 2 (SMBv2) is now supported (SMBv1 is still configurable).

Guest Portals: FortiCloud support (443300)

FortiCloud now offers the ability to manage AP's, effectively replacing the need for a physical FortiGate for customers who don't need its full set of features. As part of the SSID configuration, FortiCloud offers an external captive portal as an authentication method.

Multiple FortiAuthenticator guest portals are supported, where the FortiAuthenticator will act as the guest portal host and RADIUS server.

Note: Two-factor authentication is *not* supported for Guest Portal with FortiCloud.

NTLMv2 support (442566)

You can optionally disable NTLMv1 in the client authentication to Windows AD server configuration under *Fortinet SSO Methods* > *SSO* > *General*.

SCEP enhancements (449810)

You can now either accept or reject SCEP renewal requests for expired and revoked certificates, as burst renewal requests from FortiGates would exhaust the FortiAuthenticator and create duplicate certificates. New checkboxes in the *Renewal* section, under *Certificate Management* > *SCEP* > *Enrollment Requests*, allow you to permit renewals after certificate revocation and/or expiration.

FSSO: Chromebook logout support for SAML SP (444110)

A new logout button is provided to Chromebook users that will sign them off, successfully terminating the FortiAuthenticator's SAML SP and the end-user's FSSO session.

This can be viewed in the *SAML SP (FSSO)* section under *Authentication* > *Self-service Portal* > *Replacement Messages*, where login and logout replacement messages for SAML authentication can be configured. The logout page can be accessed and configured by going to `https://<FAC IP or FQDN>/saml-auth/logout/`.

Included in these settings is a successful logout replacement message, which confirms to end-users that the logout was successful.

Note: If you wish to redirect users to another URL upon a successful logout, you can replace specially-inserted placeholder text with the desired URL.

The following placeholder text can be found in the HTML section of *SAML SP Logout Success Page*:

```
<!-- For some providers it is possible to clear the SAML
iDP session just by redirecting the user directly to a
logout page. You can accomplish this by replacing the src
URL in the hidden iframe below. E.g.: Google:
https://accounts.google.com/Logout Okta:
https://yourdomain.okta.com/login/signout -->
```

Upgrade Instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

Hardware & VM support

FortiAuthenticator 5.1.0 supports:

- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000C
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000B
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, and Xen)

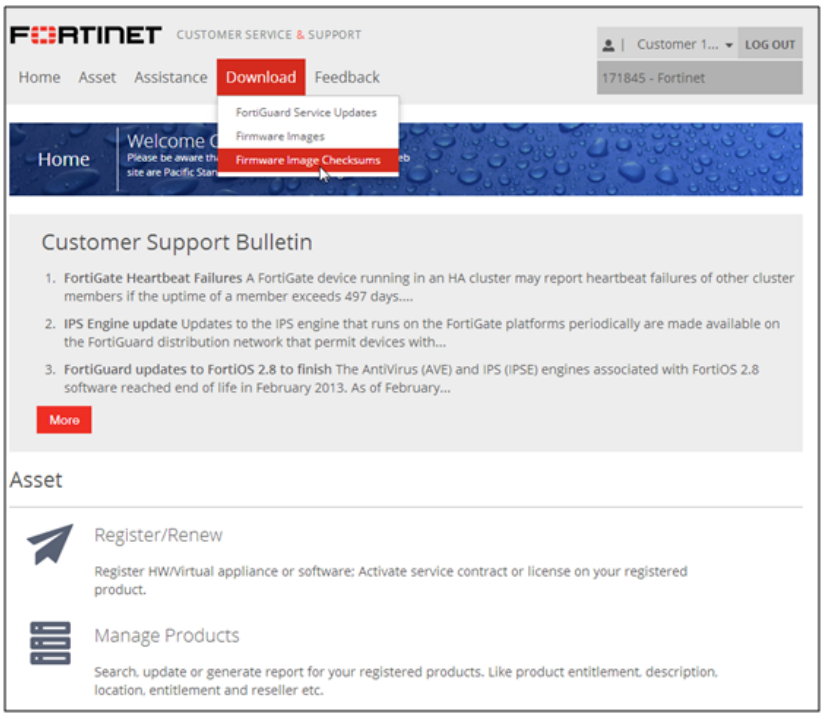
Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from Fortinet Customer Service & Support:

https://support.fortinet.com

Customer Service & Support image checksum tool



After logging in to the web site, in the menus at the top of the page, click *Download*, then click *Firmware Image Checksums*.

Alternatively, near the bottom of the page, click the *Firmware Image Checksums* button. (The button appears only if one or more of your devices has a current support contract.) In the *File Name* field, enter the firmware image file name including its extension, then click *Get Checksum Code*.

Upgrading from FortiAuthenticator v4.0

FortiAuthenticator™ 5.1.0 build 0083 officially supports upgrade from all versions of FortiAuthenticator 4.x.x.

Upgrading the FortiAuthenticator-3000D from 4.0.x to 4.1.x is not supported. The workaround for this model is to upgrade from any 4.0.x version directly to 4.2.0 or higher (skipping all 4.1.x versions).

If you install 4.1.x firmware on a FortiAuthenticator-3000D it stops responding. You can get the system running again by restoring valid firmware using the TFTP boot process.

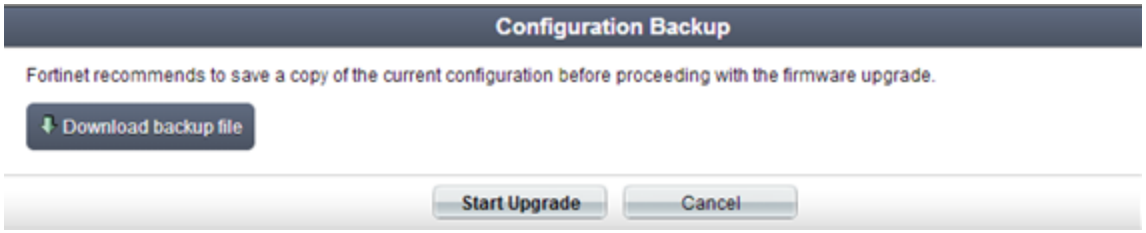
Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware package from the Customer Service & Support web site, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Customer Service & Support web site at https://support.fortinet.com. In the Download section of the page, select the Firmware Images link to download the firmware.
2. To verify the integrity of the download, go back to the Download section of the login page, then click the *Firmware Image Checksums* link.
3. Log in to the FortiAuthenticator unit's Web-based Manager using the *admin* administrator account.
4. Go to *System* > *Dashboard* > *Status*.
5. In the *System Information* widget, in the *Firmware Version* row, select *Upgrade*. The *Firmware Upgrade* or *Downgrade* dialog box opens.
6. In the *Firmware* section, select *Choose File*, and locate the upgrade package that you downloaded.
7. Select *OK* to upload the file to the FortiAuthenticator.

Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



It is recommended that a system backup is taken at this point. Once complete, click *Start Upgrade*.

Wait until the unpacking, upgrade and reboot process completes (usually 3-5 minutes), then refresh the page.

Product Integration and Support

Web browser support

The following web browsers are supported by FortiAuthenticator™ 5.1.0:

- Microsoft Internet Explorer versions 9 to 11
- Microsoft Edge 38
- Mozilla Firefox versions 18 to 54
- Google Chrome versions 28 to 59 (see note below)

Special Note for Google Chrome users

There is a known bug which exists in Google Chrome versions 44 and 45 where initially the GUI loads correctly, however after some time, pages will stop loading with the error on the chrome debug console *"Failed to load resource: net::ERR_INSECURE_RESPONSE"*.

This is a known issue and affects all sites using self-signed certificates and is fixed in Google Chrome version 46. Chrome bug reference: https://code.google.com/p/chromium/issues/detail?id=516808

To work around this issue in the meantime, use a different browser or Upgrade to the Chrome Beta Channel.

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator™ 5.1.0 supports the following FortiOS versions:

- FortiOS v5.2.11
- FortiOS v5.4.5
- FortiOS v5.6.0

Other FortiOS versions may function correctly, but may not be supported by Fortinet.

Fortinet agent support

FortiAuthenticator™ 5.1.0 supports the following Fortinet Agents:

- FortiClient v.5.x for Microsoft Windows (Single Sign-On Mobility Agent)
- FortiAuthenticator Agent for Microsoft Windows 2.0.2

- FortiAuthenticator Agent for Outlook Web Access 1.4.0
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but may not be supported by Fortinet.

For details of which Operating Systems are supported by each Agent, please see the Install Guides provided with the software.

Virtualization software support

FortiAuthenticator™ 5.1.0 supports:

- VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1, 5.5 and 6.0
- Microsoft Hyper-V 2010 and Microsoft Hyper-V 2012 R2
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM and AWS)

Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See Appendix A: FortiAuthenticator VM for more information.

Third party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor
- Token Passcode Appended - Supports any RADIUS compatible system

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS). For more information, see the FortiAuthenticator Two-Factor Authentication Interoperability Guide.

Resolved Issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please Fortinet Customer Service & Support:

https://support.fortinet.com.

This patch release fixes the following issues found in the release of 5.0.0.

Bug ID	Category	Description
448560	**Admin GUI**	Cannot create user groups.
384874	**Admin GUI**	B0081: unable to login to FortiAuthenticator GUI.
454046	**Admin GUI**	Expanding OU node on Remote LDAP server often produces the following error: Query failed: 'NoneType' object is not iterable.
452778	**Admin GUI**	Custom dictionary breaks GUI login.
449300	**Admin GUI**	Set password email link expires after 1 day when creating local users from CSV import.
449111	**Admin GUI**	Creating new user with random password fails.
437735	**Admin GUI**	"Token Resend" gives successful message by mistake.
439458	**Admin GUI**	The rad_accounting daemon doesn't restart (or reload config) when"expire inaction accounting sessions" timeout is changed.
416807	**Admin GUI**	The test filter viewing can't display all LDAP entries.
439841	**Admin GUI**	Custom RADIUS dictionary does not support pre-defined attribtue values.
434426	**Admin GUI**	Deleting a custom radius vendor returns success message stating that N vendors have been deleted (where N = # of attributes + 1).
451283	**Admin GUI**	SAML SP: Inaccurate mouse-over help text.
451002	**Admin GUI**	Remove references to Meru.
439629	**Admin GUI**	Guest user creating handles the error ungracefully.
434595	**Admin GUI**	When creating guest users fails due to invalid CSV file, the error message gets hidden because the focus of the page changes.
438476	**Admin GUI**	Admin options are displayed in remote users.

Bug ID	Category	Description
437875	**Admin GUI**	Cannot cancel/close guest user creation dialog.
439969	**Admin GUI**	Invalid file in radius vendor creation gives Django error.
440255	**Admin GUI**	GUI Packet Capture not working.
399856	**Admin GUI**	Error message on login page should not say 'All fields are case-sensitive' since the Username field isn't.
439465	**Admin GUI**	Can't login to GUI after some time in FAC 5.0.
436525	**Admin GUI**	User DN Field limit to 255 characters.
438396	**Captive Portal**	NAS not allowed for access point's IP configured for authentication for credentials portal.
440645	**Certificate Management**	UTF8 support in Certificates.
442176	**FSSO**	SSO failed to connect to LDAP server.
435530	**FSSO**	Delay in SSO session Creation (Logon Cache update) on FAC using DC Agent Mode.
446273	**FSSO**	Not able to retrieve Global Catalog database in "Fortigate Filtering" under FSSO Method.
444655	**FSSO**	SSO User Session Disappear from the SSO User Session list.
450110	**FSSO**	Lower default LDAP server response timeout.
438225	**FTM**	RADIUS initiated Push not working.
447103	**FTM**	FAC sending token activation email after FortiCare returns error.
452856	**Guest Portal**	Show guest portal URL on config page.
439038	**Guest Portal**	Remaining bugs in self-registration service of guest portal.
451455	**Guest Portal**	Guest portal troubleshooting help.
451454	**Guest Portal**	Mouse over for guest portal pre/post-login services.
451448	**Guest Portal**	Typo in log error message when Guest Portal profile is not fount.
440609	**Guest Portal**	B0012: FAC Guest Portal Rules configuration appears incomplete.
442900	**HA**	Remote Radius Administrator causing HA Sync anomalies with LB Slave.

Bug ID	Category	Description
439823	**HA**	HA our of Synch with FortiAuthenticator.
417312	**HA**	Disabling HA on low-priority FAC in HA cluster fails.
440206	**HA**	Enabling HA on FAC with several thousand remote LDAP users causes the FAC to become unresponsive.
446989	**HA**	Stale user data can interfere with LB sync or rebuild tables.
452419	**RADIUS Authentication**	[TKT – 2328649] Voice VLAN is not injected by Radius Attribute on MAB.
435094	**RADIUS Authentication**	FAC Version 4.3.2 Build 222 MAC Authentication Bypass does not work with DELL Switch N-Series.
444206	**RADIUS Authentication**	Certificate parsing fails during 802.1x authentication if there is a forward slash in the OU.
437312	**REST API**	Random password expires immediately when local user created via REST API.
404797	**REST API**	Uncalled for Push is sent after invoking auth api call.
443935	**SCEP**	B0226: Under lab. stress, GUI display "An error has occurred". Probable database connection exhaustion error.
447745	**SCEP**	B0226: SCEP renewal anomalies.
440338	**SCEP**	B0012: SCEP enrollment doesnt work - cant generate certificate from FMG.
450068	**Security**	FortiAuthenticator - tcpdump need upgrade to 4.9.2.
452483	**Security**	Release of dnsmasq-2.78, fixes CVE-2017-14491.
423286	**Security**	Advisory: Using X-XSS-Protection HTTP secure header block reflected XSS attacks.
416921	**Security**	CVE-2016-10229 Linux Kernel ipv4/udp.c Remote Code Execution Vulnerability.
413933	**Security**	Unify Web Server Banner among FortiProducts.
409889	**Security**	CVE-2017-6214 Linux Kernel "tcp_splice_read()" Denial of Service Vulnerability.
401618	**Security**	Kernel: Signed overflows in SO_{SND|RCV}BUF in sock_setsockopt().
441283	**Security**	FreeRADIUS vulnerabilities - July 17, 2017 (CVE-2017-10978, CVE-2017-10979).

Bug ID	Category	Description
441022	**Security**	Apache httpd need upgrade to 2.4.27.
452513	**SMS**	FortiGuard SMS not working.
408883	**SMS**	SMS with third party vendors generates errors for other HTTP status code than 200.
434597	**Sponsor Portal**	Sponsor user cannot download debug error report.
392437	**SSH**	B0081: SSH FAC login fails using CHAP/MS.CHAP/MS.CHAPv2 authentication to Cisco ACS remote radius users.
452545	**Usage Profile**	rad_accounting not starting when enabling usage profile feature.
439303	**Xen VM**	Openvpn and message-based debug didn't work on AWS VM.

Known Issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Category	Description

Appendix A: FortiAuthenticator VM

FortiAuthenticator VM system requirements

The following table provides a detailed summary on FortiAuthenticator VM system requirements. Installing FortiAuthenticator VM requires that you have already installed a supported virtual machine (VM) environment. For details, see the *Install Guide for FortiAuthenticator VM* available at http://docs.fortinet.com.

VM Requirements

Virtual Machine	Requirement
Virtual Machine Form Factor	Open Virtualization Format (OVF)
Virtual CPUs Supported (Minimum / Maximum)	1 / 8
Virtual NICs Supported (Minimum / Maximum)	1 / 4
Storage Support (Minimum / Maximum)	60GB / 2TB
Memory Support (Minimum / Maximum)	512 MB / 64GB
High Availability Support	Yes

FortiAuthenticator VM firmware

Fortinet provides FortiAuthenticator VM firmware images in two formats:

- **.out**
  Use this image for new and upgrades to physical appliance installations. Upgrades to existing virtual machine installations are also distributed in this format.
- **ovf.zip**
  Use this image for new VM installations. It contains a deployable Open Virtualization Format (OVF) virtual machine package for initial VMware ESXi installations.

For more information see the FortiAuthenticator product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortiauthenticator/index.html.

Appendix B: Maximum values

This section lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware and VM configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Hardware appliances

The following table describes the maximum values set for the various hardware models.

Feature		FortiAuthenticator Model				
		200E	400E	1000D	2000E	3000E
System						
Network	Static Routes	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20
	SMS Gateways	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20
Administration	SYSLOG Servers	20	20	20	20	20
	User Uploaded Images	30	100	500	1000	2000
	Language Files	50	50	50	50	50
Realms		20	80	400	800	1600
Authentication						
General	Auth Clients (NAS)	166	666	3333	6666	13333

Feature		FortiAuthenticator Model				
		200E	400E	1000D	2000E	3000E
	Users (Local + Remote)[1]	500	2000	10000	20000	40000
	User Radius Attributes	1500	6000	30000	60000	120000
	User Groups	50	200	1000	2000	4000
	Group Radius Attributes	150	150	600	6000	120000
	FortiTokens	1000	4000	20000	40000	80000
	FortiToken Mobile Licenses[2]	200	200	200	200	200
	LDAP Entries	1000	4000	20000	40000	80000
	Device (MAC-based Auth.)	50	200	1000	2000	4000
	RADIUS Client Profiles	500	2000	10000	20000	40000
	Remote LDAP Servers	20	80	400	800	1600
	Remote LDAP Sync Rule	25	100	500	1000	2000
	Remote LDAP User Radius Attributes	1500	6000	30000	60000	120000
FSSO & Dynamic Policies						
FSSO	FSSO Users	500	2000	10000	20000	200000[3]
	FSSO Groups	1000	1000	5000	10000	20000
	Domain Controllers	10	20	100	200	400
	RADIUS Accounting SSO Clients	166	666	3333	6666	13333
	FortiGate Services	50	200	1000	2000	4000
	FortiGate Group Filtering	250	1000	5000	10000	20000
	FSSO Tier Nodes	5	20	100	200	400
	IP Filtering Rules	250	1000	5000	10000	20000

Feature		FortiAuthenticator Model				
		200E	400E	1000D	2000E	3000E
Accounting Proxy	Sources	500	2000	10000	20000	40000
	Destinations	25	100	500	1000	2000
	Rulesets	25	100	500	1000	2000
Certificates						
User Certificates	User Certificates	2500	10000	50000	100000	200000
	Server Certificates	50	200	1000	2000	4000
Certificate Authorities	CA Certificates	10	10	50	50	50
	Trusted CA Certificates	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200
SCEP	Enrollment Requests	2500	10000	50000	100000	200000

[1] Note that there is one metric used for the number of allowed users which is *Users*. Local Users and Remote Users share the same limit value. This enables Local Users ***or*** Remote Users to be equal to *Users* or for there to be a mixture of user types, however, the total number of Local and Remote Users cannot exceed the *Users* metric.

[2] *FortiToken Mobile Licenses* refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E, the total number of concurrent SSO Users is set to a higher level to cater for large deployments.

VM appliances

The FortiAuthenticator-VM Appliance is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator VM-Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The Calculating Metric column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator-VM Base License, the number of Auth Clients (NAS Devices) that can authenticate to the system is:

100 / 10 = 10

Where this relative system is not used e.g. for static routes, the *calculating metric* is denoted by a '-'. The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Maximum Values - Virtual Machines

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	SYSLOG Servers	2	20	20	20
	User Uploaded Images	5	Users / 20	5	100
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (NAS)	3	Users / 3	33	1666
User Management	**Users** (Local + Remote)[1]	5	**********	100	5000
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	Users x 3	300	15000
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) [2]	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	1	Users / 10	10	500

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
	RADIUS Client Profiles	3	Users	100	10000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Sync Rule	1	Users / 20	5	250
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	30	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users /100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
Accounting Proxy	Sources	3	Users	100	1000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500

Feature		Model			
		Unlicensed VM	Calculating Metric	Base VM (100 Users)	Example 5000 licensed User VM
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	200	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	2500	10000

[1] Note that there is one metric used for the number of allowed users which is *Users*. Local Users and Remote Users share the same limit value. This enables Local Users ***or*** Remote Users to be equal to *Users* or for there to be a mixture of user types, however, the total number of Local and Remote Users cannot exceed the *Users* metric.

[2] *FortiToken Mobile Licenses* refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

FORTINET®

High Performance Network Security